anand guru

SOC EXPERTS

Interview Questions on **Threat Hunting**

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Threat Hunting?

Threat hunting is a human-driven, proactive and iterative approach which involves searching through networks & endpoints, to detect malicious activities that have evaded detection by existing automated tools.

Hunting is an offense-based approach that applies adversaries' tactics and techniques, and adopts their mindset when investigating signs of compromise within an organization.

anand guru

anand guru

Explain Threat Hunting Process.

The process involves 5 stages

1 - Hypothesis Generation: The aim of these hypotheses is to find evidence of threats before they are exploited, or even ones that are already being exploited.

2 – Validation of the hypotheses: Once a hypothesis has been defined, its validity needs to be verified. We then need to look for the existence of threats that fit this hypothesis. In this stage it is usual for some hypotheses to be discarded, while research into others is prioritized due to their likelihood or criticality.

3 – Finding evidence: From the results obtained in the previous search, we need to verify if a threat really exists. False positives and mistakes in configuration are set aside, and efforts are focused on the validated hypotheses.

4 – Discovery of new patterns: The attack is reconstructed to find any new patterns and tactics used to carry it out.

5 – Notification and enrichment: Using the knowledge generated during the Threat Hunting process, the automatic detection systems are enriched and improved. This way, the organization's global security is improved.

anand guru

anand guru

Why should we do Threat Hunting?

Advantages of threat hunting are as follows:

- Proactively Uncover Security Incidents
- Detect the undetected
- Improve the Speed of Threat Response
- Reduces False Positives and Improves SOC Efficiency
- Reduce dwell time. Hunting enables an organization to identify and stop adversaries early in the kill chain stops them from reaching their ultimate target.
- Evict adversaries with minimal business disruption.

anand guru

anand guru

Difference between Threat Hunting and Threat Detection?

Threat Detection is a reactive approach.

Use traditional preventive technologies and monitoring tools to detect a malicious activity.

Threat detection leads to mitigation.

Threat Hunting is a proactive approach.

Detect slow and stealth attacks that would otherwise go unnoticed by preventive technologies.

Threat hunting leads to threat detection and incident response.

anand guru

anand guru

What tools do you use for Threat Hunting.

Few of the threat hunting tools are

- **Sqrrl**
- **Vectra Cognito**
- **Exabeam Threat hunter**
- **Endgame**
- **DNIF**

Other tools that help during threat hunting include

- **EDR**
- **Threat Intelligence**
- **ELK for analytics**

anand guru

anand guru

Explain the different Threat Hunting Techniques.

Different thereat hunting techniques are as follows:

Searching: This is probably the most basic form of threat hunting. With this technique, you are trying to support your formulated hypothesis with information and data from a very specific set of defined search criteria

Clustering: This is more of a quantitative, statistically-based approach to threat hunting. With this technique, the threat hunter is attempting to “cluster” similar datasets from a larger pool of data, to find the hidden or unseen trends in these datasets

Grouping: In this scenario, the threat hunter is looking at different (or unique) artifacts that have been discovered and identifying them based on the same set of criteria that was used to formulate the original hypothesis

Stack Counting: This is another type of statistical technique. In this case, the threat hunter ascertains the total number of occurrences of a certain dataset by closely examining any sorts of outliers that may exist

anand guru

anand guru

Explain the OODA Strategy.

OODA is an abbreviation of Observe, Orient, Decide and Act. Military personnel apply OODA when they carry out combat operations. Likewise, threat hunters use OODA during cyberwarfare. In the context of threat hunting, OODA works as:

Observe: A first phase that involves routine data collection from endpoints

Orient: Understanding the collected data thoroughly and combining this information with other collected information to help understand its meaning.

Decide: Once you have analyzed the information, then you need to identify the course of action. If the incident occurs, threat hunters will execute the incident response strategy

Act: The last phase involves the execution of the plan to put an end to the intrusion and enhance the company's security posture. Further measures are taken to prevent the same type of attack in the future

anand guru

anand guru

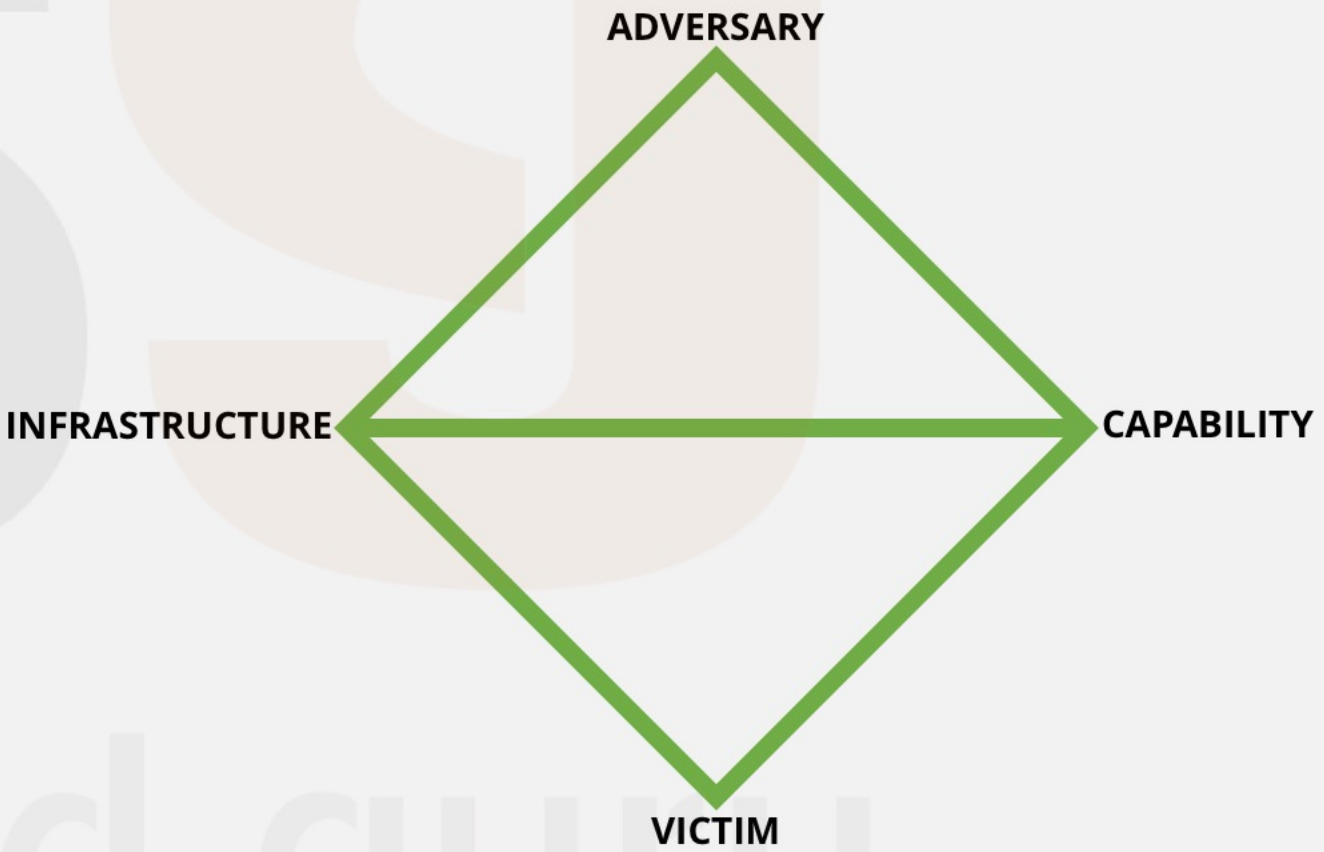
What is Diamond Model?

The Diamond Model emphasis the relationship between basic elements of any malicious activity.

It has 4 elements

1. **The Adversary**
2. **The Victim**
3. **Infrastructure**
4. **Capability**.

All malicious activity contains these elements.



anand guru

anand guru

What is MITRE ATT&CK? How is it used in Threat Hunting?

ATT&CK stands for Adversarial Tactics, Techniques and Common Knowledge.

It is a knowledge base of the attacks, the tactics and techniques used and associated APT groups.

It helps in mapping out an attack in various stages (called Tactics) and methods/tools (called Techniques) used at various stages.

MITRE ATT&CK framework is used by threat hunters

- To map various attack vectors.
- Identify the ones that your organization is susceptible to.
- Build hypothesis around the prioritized techniques.
- Hunt for the adversaries.

anand guru

anand guru

Give example of Threat Hunting Hypothesis.

1. Recognizing suspicious software

- This is useful in detecting malwares.
- Look for Event ID **4688**. Also use **sysmon** to enable logging of all process start and termination.
- Make a list of all standard processes that run in the network.
- Use process Hashes (some malwares can run with legit process names (like notepad.exe)

2. Detecting Command and Control Communication

- Malware communicate back to C2 servers for exfiltration data or get further instructions for the attack.
- They typically use common port number to avoid detection. But we can check for various combination of communication channels like:
  - Common Port & Common Protocol
  - Common Port & Uncommon Protocol
  - Uncommon Port & Common Protocol
  - Uncommon Port & Uncommon Protocol
- Hypothesis: Attackers may be operating on a C2 channel that uses a common protocol on a common network port
  - Look for unique artifacts pertinent to the protocol you are interested in. For example, if you are interested in identifying C2 in HTTP traffic, then you might consider looking for anomalous domains/URLs/User-Agent strings.
- Dataset to use:
  - HIPS logs
  - Firewall Logs
  - Proxy Logs
  - DNS Logs

anand guru

anand guru

Example of Threat Hunting Hypothesis.

3. Hunting for Internal Reconnaissance

Hypothesis: An attacker conducting internal reconnaissance would attempt to carry out host enumeration and automate these commands with a script

Look for these commands to be spawned by a script:

- whoami
- net user
- useraccount (WMIC)
- Get-NetIPConfiguration (PowerShell)
- hostname
- ipconfig
- nicconfig (WMIC)

Dataset to use:

- Process Names
- Process Hashes

anand guru

anand guru

What makes a person good at Threat Hunting?

- Good understanding of various attack vectors (TTPs in ATT&CK framework)
- Hypothetical thinking: the ability to hypothesize threat attacks, source vectors, and organizational impact
- Good knowledge of organization infrastructure
- Good at pattern recognition
- Being aware of latest attack techniques
- Data Analytics
- Basic scripting knowledge for automation

anand guru

anand guru

How do you measure effectiveness of Threat Hunting?

Few of the key metrics in measuring effectiveness of threat hunting include:

- Number of incidents by severity
- False positive rate of transitioned hunts
- Dwell time of any incidents discovered
- Number of detection gaps identified and fixed
- Logging gaps identified and corrected
- Insecure practices identified and corrected
- Number of hunts transitioned to new analytics
- Any new visibility gained

anand guru

anand guru

Full course on Udemy

IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

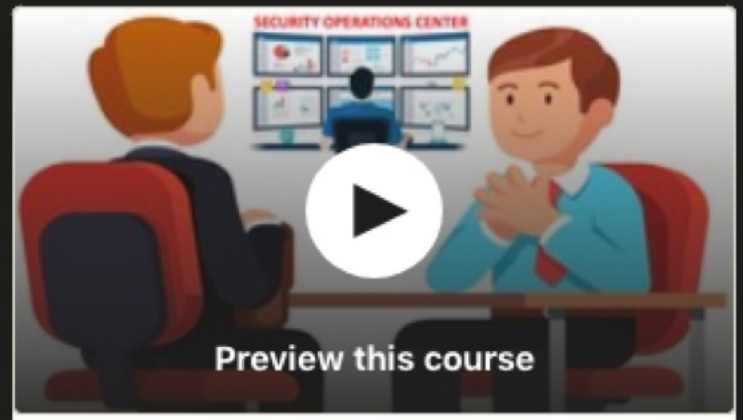
Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★½ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

Wishlist Share Gift this course



₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

Add to cart

Buy now

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion